UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/036,897	12/26/2001	Vladimir S. Zaborovsky	FRACX 100	5179

7590 02/06/2007

Jason H. Foster
Kremblas, Foster, Phillips & Pollick
7632 Slate Ridge Blvd.
Reynoldsburg, OH 43068

EXAMINER	
FIELDS, COURTNEY D	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/036,897	ZABOROVSKY ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claim 2 has been cancelled.

2. Claim 9 has been added.

3. Claims 1 and 3-9 are pending.

Response to Arguments

4. Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection, in view of Droz et al. (U.S. Patent No. 6,950,946).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1 and 3-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baehr et al. (US Patent No. 5,878,231) in view of Droz et al. (U.S. Patent No. 6,950,946).

Regarding claim 1, Baehr et al. discloses an apparatus and method for providing a secure firewall between a private network and a public network. The apparatus combined with a computer network for packets delivery with headers that contain logical and physical addresses of at least one of the sender and the receiver of information (See Column 5, lines 61-77, Column 6, lines 1-19), the apparatus comprising: a network screen connected to the computer network and through which the packets pass (See

Column 2, lines 10-24), wherein the network screen splits the computer network into at least two segments, has hardware and software means, and at least two network interfaces by which the network screen connects to the computer network for packets exchange between the network segments (See Column 3, lines 17-30 and Column 9, lines 15-17), wherein the software controls the process of packets commutation between the network interfaces based on a set of filtration rules (See Column 9, lines 15-30), does not name logical addresses to the segments, and at the same time the software permits transit delivery through the network interfaces only to those packets with headers that meet the filtration rules (See Column 5, lines 61-77, Column 6, lines 1-19, and Column 9, lines 46-53)

However, Baehr et al. fails to explicitly disclose the feature wherein the network interfaces based on a set of filtration rules does not send physical addresses to the computer network. Droz et al. discloses a network-attachable computer system for generating identity information comprising a secure identifier and a key, to determine whether the computer system has been lost or stolen based upon the packet filter rules. (See Droz et al., Column 9, lines 11-45) The physical address (MAC) is hidden within a file or a hard disk partition stored within the computer (See Droz et al., Column 7, lines 60-64)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Baehr et al.'s packet filtration system with Droz et al.'s protection mechanism. Motivation for such an implementation would enable the identity of the physical address within the network to remain unknown to the intruder by

incorporating a network screen which is protected by using an encryption key (See Droz et al., Column 3, lines 36-49)

Regarding claim 3, (Baehr et al. as modified by Droz et al.) discloses the claimed limitation wherein the network screen is based on a universal computer device having an operating system, more than two network interfaces and special direct interface for editing the filtration rules (See Baehr et al., Column 3, lines 17-30 and Column 9, lines 15-17)

However, Baehr et al. fails to explicitly disclose the feature wherein the network interfaces based on a set of filtration rules does not send physical addresses to the computer network. Droz et al. discloses a network-attachable computer system for generating identity information comprising a secure identifier and a key, to determine whether the computer system has been lost or stolen based upon the packet filter rules. (See Droz et al., Column 9, lines 11-45) The physical address (MAC) is hidden within a file or a hard disk partition stored within the computer (See Droz et al., Column 7, lines 60-64)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Baehr et al.'s packet filtration system with Droz et al.'s protection mechanism. Motivation for such an implementation would enable the identity of the physical address within the network to remain unknown to the intruder by incorporating a network screen which is protected by using an encryption key (See Droz et al., Column 3, lines 36-49)

Regarding claim 4, (Baehr et al. as modified by Droz et al.) discloses the claimed limitation wherein the filtration rules of the network screen disallow a transit delivery of any messages that do not have special mark and address parameters in their headers (See Baehr et al., Column 10, lines 1-34)

However, Baehr et al. fails to explicitly disclose the feature wherein the network interfaces based on a set of filtration rules does not send physical addresses to the computer network. Droz et al. discloses a network-attachable computer system for generating identity information comprising a secure identifier and a key, to determine whether the computer system has been lost or stolen based upon the packet filter rules. (See Droz et al., Column 9, lines 11-45) The physical address (MAC) is hidden within a file or a hard disk partition stored within the computer (See Droz et al., Column 7, lines 60-64)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Baehr et al.'s packet filtration system with Droz et al.'s protection mechanism. Motivation for such an implementation would enable the identity of the physical address within the network to remain unknown to the intruder by incorporating a network screen which is protected by using an encryption key (See Droz et al., Column 3, lines 36-49)

Regarding claim 5, (Baehr et al. as modified by Droz et al.) discloses the claimed limitation wherein access to the program of editing the filtration rules is protected by password (See Baehr et al., Column 5, lines 38-52)

However, Baehr et al. fails to explicitly disclose the feature wherein the network interfaces based on a set of filtration rules does not send physical addresses to the computer network. Droz et al. discloses a network-attachable computer system for generating identity information comprising a secure identifier and a key, to determine whether the computer system has been lost or stolen based upon the packet filter rules. (See Droz et al., Column 9, lines 11-45) The physical address (MAC) is hidden within a file or a hard disk partition stored within the computer (See Droz et al., Column 7, lines 60-64)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Baehr et al.'s packet filtration system with Droz et al.'s protection mechanism. Motivation for such an implementation would enable the identity of the physical address within the network to remain unknown to the intruder by incorporating a network screen which is protected by using an encryption key (See Droz et al., Column 3, lines 36-49)

Regarding claim 6, (Baehr et al. as modified by Droz et al.) discloses the claimed limitation wherein the network screen after processing the packet with the filtration rules keeps unchanged the logical and physical addresses of the sender in the packet's header and the network screen does not name network interfaces with logical addresses and the network screen contains a special direct interface connected thereto to edit the filtration rules and any changes of filtration rules may be processed only through this interface and the program of control provides packet delivery from one network interface to another only when the information in the packet's header satisfies

all filter requirements (See Baehr et al., Column 5, lines 61-77, Column 6, lines 1-19, and Column 9, lines 46-53)

However, Baehr et al. fails to explicitly disclose the feature wherein the network interfaces based on a set of filtration rules does not send physical addresses to the computer network. Droz et al. discloses a network-attachable computer system for generating identity information comprising a secure identifier and a key, to determine whether the computer system has been lost or stolen based upon the packet filter rules. (See Droz et al., Column 9, lines 11-45) The physical address (MAC) is hidden within a file or a hard disk partition stored within the computer (See Droz et al., Column 7, lines 60-64)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Baehr et al.'s packet filtration system with Droz et al.'s protection mechanism. Motivation for such an implementation would enable the identity of the physical address within the network to remain unknown to the intruder by incorporating a network screen which is protected by using an encryption key (See Droz et al., Column 3, lines 36-49)

Regarding claim 7, (Baehr et al. as modified by Droz et al.) discloses the claimed limitation wherein the network screen is a special computer device with an interface operating system universal bus for data exchange with the interfaces and a separate channel of control protected by password (See Baehr et al., Column 5, lines 38-52)

However, Baehr et al. fails to explicitly disclose the feature wherein the network interfaces based on a set of filtration rules does not send physical addresses to the

computer network. Droz et al. discloses a network-attachable computer system for generating identity information comprising a secure identifier and a key, to determine whether the computer system has been lost or stolen based upon the packet filter rules. (See Droz et al., Column 9, lines 11-45) The physical address (MAC) is hidden within a file or a hard disk partition stored within the computer (See Droz et al., Column 7, lines 60-64)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Baehr et al.'s packet filtration system with Droz et al.'s protection mechanism. Motivation for such an implementation would enable the identity of the physical address within the network to remain unknown to the intruder by incorporating a network screen which is protected by using an encryption key (See Droz et al., Column 3, lines 36-49)

Regarding claim 8, (Baehr et al. as modified by Droz et al.) discloses the claimed limitation wherein a special direct interface to define the filtration rules (See Baehr et al., Column 6, lines 37-59)

However, Baehr et al. fails to explicitly disclose the feature wherein the network interfaces based on a set of filtration rules does not send physical addresses to the computer network. Droz et al. discloses a network-attachable computer system for generating identity information comprising a secure identifier and a key, to determine whether the computer system has been lost or stolen based upon the packet filter rules. (See Droz et al., Column 9, lines 11-45) The physical address (MAC) is hidden within a

file or a hard disk partition stored within the computer (See Droz et al., Column 7, lines 60-64)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Baehr et al.'s packet filtration system with Droz et al.'s protection mechanism. Motivation for such an implementation would enable the identity of the physical address within the network to remain unknown to the intruder by incorporating a network screen which is protected by using an encryption key (See Droz et al., Column 3, lines 36-49)

Regarding claim 9, (Baehr et al. as modified by Droz et al.) discloses the claimed limitation wherein packets outbound from the device through one of the network interfaces retain in their headers physical address of the at least one sender of the packets by the program that controls the network screen not communicating the physical addresses of its network interfaces (See Droz et al., Column 9, lines 56-67 and Column 10, lines 1-9)

However, Baehr et al. fails to explicitly disclose the feature wherein the network interfaces based on a set of filtration rules does not send physical addresses to the computer network. Droz et al. discloses a network-attachable computer system for generating identity information comprising a secure identifier and a key, to determine whether the computer system has been lost or stolen based upon the packet filter rules. (See Droz et al., Column 9, lines 11-45) The physical address (MAC) is hidden within a file or a hard disk partition stored within the computer (See Droz et al., Column 7, lines 60-64)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Baehr et al.'s packet filtration system with Droz et al.'s protection mechanism. Motivation for such an implementation would enable the identity of the physical address within the network to remain unknown to the intruder by incorporating a network screen which is protected by using an encryption key (See Droz et al., Column 3, lines 36-49)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
January 25, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER